Security Standard – Malware Protection (SS-015)

Chief Security Office

Date: 09/02/2023

Department for Work & Pensions

This Malware Protection Security Standard is part of a suite of standards, designed to promote consistency across the Authority, and supplier base with regards to the implementation and management of security controls. For the purposes of this standard, the term DWP and Department are used interchangeably.

Security standards and policies considered appropriate for public viewing are published here:

https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards

Technical security standards cross-refer to each other where needed, so can be confidently used together. They contain both mandatory and advisory elements, described in consistent language (see table below).

Table 1 – Terms

Term	Intention
must	denotes a requirement: a mandatory element.
should	should denotes a recommendation: an advisory element.
may	denotes approval.
might	denotes a possibility.
can	denotes both capability and possibility.
is/are	is/are denotes a description.

2. Revision history

Version	Author	Description	Date
1.0		First published version	20/03/2017
2.0		Full update in line with current best practices and standards; • Updated Intro, purpose, audience, scope • Written to be vendor and technology agnostic as far as possible to increase applicability • Replaced use of technical control requirements to minimum security measures • Re-formatted document to categorise security measures under 15 headings. • Added NIST sub-category references against each security measure • Added new table in Appendix A which list security outcomes the measures support the achievement of • Updated references and included links to external publications etc. 11.1.2 Updated regarding use of open source anti-malware 11.2 New section for privileged users 11.5.2 Added caveat for special users 11.8.1 File transfer restrictions in instant messaging 11.10.3 Requirement added for sandboxing 11.13.5 Block C&C traffic	09/02/2023

3. Approval history

Version	Name	Role	Date
1.0		Chief Security Officer	18/09/2017
2.0		Chief Security Officer	09/02/2023

This document will be reviewed for continued completeness, relevancy, and accuracy within 1 year of being granted "final" status, and at yearly intervals thereafter.

4. Compliance

Security assurance teams will verify compliance with this standard through various methods, including but not limited to, internal and external audits, and feed back to the appropriate Authority Risk and System Owner.

5. Exceptions Process

In this document the term **"must"** is used in bold letters to indicate a mandatory security measure. Any exceptions to the application of this standard, or where specific security measures cannot be adhered to, **must** be presented to the Authority. This **must** be carried out prior to deployment and managed through the design caveats or exception process.

Such exception requests will invoke the Risk Management process to clarify the potential impact of any deviation to the configuration detailed in this standard.

Exceptions to the standard **must** be maintained on a risk register for accountability, traceability, and security governance reporting to senior management.

6. Audience

This document is intended for, but not necessarily limited to, technical architects, engineers, developers, security teams, project teams, including suppliers engaged in the design, development, implementation and operation of systems, services and applications that require malware protection.

7. Accessibility statement

Users of this standard **must** consider accessibility design requirements as appropriate. Further information on accessibility standards can be found in Appendix F.

8. Introduction

This Malware protection Security Standard provides the list of security measures that are required to secure User Access Devices, Servers and infrastructure components to an Authority approved level of security. This standard provides a list of security measures to protect citizen and operational data to be stored or processed in order to minimise the risk from known threats both physical and logical to an acceptable level for operations.

Quoting NIST (National Institute of Standards and Technology) the definition of malware is:
“Malware, also known as malicious code, refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim’s data, applications, or operating system.
Malware is the most common external threat to most hosts, causing widespread damage and disruption and necessitating extensive recovery efforts within most organizations.”

There are several use cases requiring malware controls and agent-based malware mitigation software **must** be considered on all End User Devices, e.g., desktop endpoints, mobile end points, along with all server end points (physical and virtual including Hypervisor) and at the content inspection and inline infrastructure layers.

Malware detection capability **must** be considered on webserver end points, mail server endpoints, remote access servers / VPN concentrators, firewalls, proxy and reverse proxy servers and intrusion prevention systems.

As this standard only provides minimum measures, they **should** be exceeded as appropriate depending on the threats and risks that need to be addressed, the sensitivity of the data, and in keeping with latest security enhancements.

The security measures are derived from industry best practice i.e. guidance published by NIST, CIS and OWASP (see Appendix C for full list external references) and support the implementation of appropriate security controls as selected by the Authority or our third party providers, such as the CIS Critical Security Controls v8 controls set. [see External References]

Every effort has been made to ensure the security measures are vendor and technology agnostic as far as possible; this is to ensure greater applicability of the standard regardless of the technologies used. The security measures **may** be implemented in different ways, depending on the technology choices and business requirements in question.

The aim of this standard is to:

- Ensure malware controls are implemented consistently across the Authority and its third-party service providers.
- Mitigate risks from the threats and vulnerabilities associated with malware to an acceptable level for operation.
- Support the achievement of security outcomes described in Appendix A.

Technical security standards ultimately support the achievement of security outcomes sought by the Authority. They set the expectations for what needs to be done to achieve them and why, and provide an objective, measurable statement of the Authority's existing security posture in a number of important areas. The outcomes are based on the official NIST sub-categories where possible to ensure close alignment with the NIST Cyber Security Framework (CSF) and are enabled by the implementation of controls from the CIS Critical Security Controls v8 controls set. [see External References]. Those relevant to the subject of each standard can be found in Appendix A of every technical security standard.

9. Purpose

The purpose of this standard is to ensure that Authority systems and services are designed, configured, deployed, and managed consistently to protect against typical threats at the OFFICIAL tier.

This standard also serves to provide a baseline in which assurance and compliance activities can be carried out, so that the Authority can be assured that security obligations are being met or exceeded.

10. Scope

This standard applies to systems deployed to meet Authority business objectives. All endpoints **must** have Anti-Malware software based agents installed to help protect against and remediate infection, and **must** meet all the requirements in this standard. The scope includes endpoints that receive auxiliary agentless anti-malware mitigation via IDS / IPS, Next Generation Sandboxing devices, and other Content Inspection devices, which **must** meet all of the logging and incident handling requirements. Any devices that are not anti-malware compatible **must** be protected by suitable compensating controls. Any queries regarding the security measures laid out in this standard **should** be sent to the Authority.

11. Minimum Technical Security Measures

The following section defines the minimum-security measures that **must** be implemented to achieve the security outcomes described in Appendix A. For ease of reference, the official NIST sub-category ID is provided against each security measure e.g., PR.PT-3, to indicate which outcome(s) it contributes towards. Refer to Appendix A for full description of outcomes.

11.1 Malware Protection Security Requirements

Reference	Minimum Technical Security Measures	NIST ID
11.1.1	When selecting Anti-Malware software and Anti-Malware Content Inspection devices during both procurement and deployment, architects **must** evaluate Anti-Malware technologies that provide similar functionality throughout the end-to-end systems architecture and select products to avoid duplication of identical scanning engines and to remove unnecessary performance overhead.	ID.AM-5 ID.RA-1
11.1.2	If open-source Anti-Malware software is chosen, clear SLA's and escalation processes **must** be defined to handle software failure, i.e., signature updates that may cause false positives and impact associated systems and service operating. (Note: Commercially available Anti-Malware will have well-defined SLAs as part of the procurement and commercial contract. Open-source Anti-Malware software will not necessarily have these in place by default, but must have a clearly defined service wrapper in place, supported by commercial agreements where appropriate.)	ID.BE-4 ID.SC-3

11.2 Privileged Users

Reference	Minimum Technical Security Measures	NIST ID
11.2.1	Privileged Users who manage Anti-Malware software, hardware, processes and services **must** be able to demonstrate having the appropriate level of training for the products, processes and services they manage.	PR.AT-2
11.2.2	Privileged Users must be managed in accordance with SS-001 pt.2 Privileged User Access Security Standard [Ref. C].	PR.AC-4
11.2.3	The principle of least privilege **must** be applied to ensure that end users only have the required access to perform their business tasks and no access to modify any system parameters on the Operating System other than for HID (Human Interface Devices) e.g., for their personal ergonomic requirements. This includes but is not limited to restricting access to system logs, driver settings, time settings, host-based firewalls, process browsers, and service management settings. Full coverage of desktop / end user operating system lockdown can be found in SS-010 Desktop Operating System Security Standard [Ref. A].	PR.AC-4

11.3 Operating System

Reference	Minimum Technical Security Measures	NIST ID
11.3.1	Operating Systems **must** be running versions that are still under active vendor support and must be patched under time sensitive operating procedures according to SS-033 Security Patching Standard [Ref. B].	ID.AM-2
11.3.2	If an Operating System is in use that is no longer under vendor support, a clear migration plan **must be** well-defined and managed. Furthermore, other mitigations to ensure clear restrictions to Internet based traffic and an adequate level of inline Content Inspection **must** be in effect. (This is because end point Anti-Malware software on these systems will not provide the required level of requisite protection).	ID.AM-1 ID.AM-2

11.4 Anti-malware software

Reference	Minimum Technical Security Measures	NIST ID
11.4.1	Standard business users **must** not have any access to modify or disable the scanning parameters of the Anti-Malware software. This includes preventing user access to disable Anti-Malware capabilities in the BIOS.	PR.AC-4 PR.PT-4
11.4.2	Access to the Anti-Malware software console **must** be protected to avoid any tampering by non-privileged users.	PR.AC-4 P.PT-4

11.4.3	Any privileged access exercised to modify Anti-Malware software scanning parameters **must** be fully logged and audited.	PR.PT-1

11.5 Browser

Reference	Minimum Technical Security Measures	
11.5.1	Standard business users **must not** have any access to modify any of the browser-based settings such as, but not limited to, privacy settings, proxy settings, Active X, and Java based settings.	PR.AT -1 PR.AC-4
11.5.2	Standard business users **must not** have the ability to install or modify any browser-based plugins. Non-production users (e.g. engineers, developers etc.) may install plugins via a request/approval process.	PR.AC-4
11.5.3	The only browser-based parameters that a standard business user **must** have access to, is for the accommodation of ergonomic requirements such as modifying the zoom feature for vision assistance.	PR.AC-4
11.5.4	Configuration on the browser **must** severely limit non-essential browsing features such as web-based popups and iFrames; any requirement or exception must be subject to security assessment and accordingly authorised.	PR.AC-4

11.5.5	Users **must**: i) only use corporately approved browsers, ii) NOT have the ability to install any non-approved browsers This is a specific clause to item 11.9.1.	PR.AC-4

11.6 Removable Storage

Reference	Minimum Technical Security Measures	
11.6.1	If removable media is authorised as part of legitimate business use, the auto-run feature **must** be disabled and an on demand Anti-Malware software scan **must** be completed and successfully passed prior to the data being persisted on department systems.	PR.DS-3 PR.DS-5
11.6.2	If removable media is authorised the device **must** be first introduced to a sand box / air gapped environment and the Anti-Malware scan complete successfully before device installation to the main corporate or supplier network.	PR.DS-3 PR.DS-5

11.7 Virtual Private Network

Reference	Minimum Technical Security Measures	
11.7.1	Any VPN Concentrators aggregating remote worker access to systems and services implemented for Authority business and services **must** perform a posture check of the devices attempting remote connectivity. This **must** include checks on patching levels, Anti-Malware software signature levels Anti-Malware software service status and confirmation that the device is appropriately authorised to access the network.	DE.CM-4, DE.CM-5 DE.CM-7 DE. DP-3
11.7.2	If remote worker end point devices do not meet posture check requirements of the VPN concentrator, there **must** be an effective facility in a quarantine / staging area to rectify patching levels, Anti-Malware software signature levels and service status in order to reattempt successful connection.	DE.CM-1 DE.CM-4 DE.CM-5 DE.CM-7 DE. DP-3

11.8 Instant Messaging

Reference	Minimum Technical Security Measures	
11.8.1	Instant Messaging channels **must** have file transfer disabled by default, and only enabled for authorised and approved users.	PR.DS-5
11.8.2	If communicating with approved federated third parties via an Instant Messaging channel, file	PR.PT-4

	transfer **must** have an on-demand scan Anti-Malware software scan enabled	DE.CM-4

11.9 General Software Controls

Reference	Minimum Technical Security Measures	
11.9.1	Standard business users **must not** have the ability to install unauthorised software on any departmental systems.	PR.AC-4
11.9.2	Endpoint controls **must** consider application whitelisting to help mitigate the deployment of unauthorised software and malware execution.	DE.CM-4
11.9.3	All approved software **must** be subject to the same patching standards as the underlying Operating System patching standards, and in line with SS-033 Security Patching Standard [Ref. B].	PR.IP-12
11.9.4	Any software found to have bypassed any control mechanisms for installation **must** be automatically disabled / quarantined and subjected to a formal review and uninstallation if deemed necessary.	PR.IP-12

11.10 File transfer controls

Reference	Minimum Technical Security Measures	
11.10.1	File Transfers **must** be subject to at least one layer of content inspection by Anti-Malware software prior to the data being resident/ persistent on department systems	DE.CM-4
11.10.2	File Transfers with approved third parties **must** be subject to at least two layers of content inspection. Where decryption is possible, this **must** be done firstly by a Security Boundary service, such as a Next Generation Firewall, Web Application Firewall, or Proxy Server, and secondly by a real time scan using the Anti-Malware software on the target end point.	DE.CM-4
11.10.3	Where file transfers are encrypted and cannot be decrypted for inspection in transit (e.g. certificate pinned files), these **must** be directed to a quarantine or sandbox environment.	DE.CM-4

11.11 Threat Intelligence

Reference	Minimum Technical Security Measures	
11.11.1	Anti-Malware threat intelligence feeds **must** be regularly collected and reviewed from known, trusted third parties. These **must** be digested by a dedicated team and distributed to relevant stakeholders for consumption.	ID.RA-3

11.12 Anti-Malware Software

Reference	Minimum Technical Security Measures	
11.12.1	Anti-Malware software **must** be installed, verified and actively running on all end points.	DE.CM-4
11.12.2	Anti-Malware software **must** have on-access (real-time) scanning enabled by default for general web browsing, file and folder download and upload via email attachments.	DE.CM-4
11.12.3	Anti-Malware software **must** have as a minimum frequency interval a weekly on-demand scan completed of the entire file and folder structure. This **must** include a scan of the start-up files, boot records and memory.	DE.CM-4
11.12.4	Where exceptions are identified, conflicts with on-access (real-time) Anti-Malware and / or on-demand scans **must** be auditable, well-defined and	DE.CM-4

	justified against a demonstrable operational requirement. Vendor documentation describing requirements for Anti-Malware software scan exceptions **must** be indexed and archived for reference, auditing and review.	
11.12.5	Anti-Malware software **must** be configured to log any malware detection to a centralised repository that is actively reviewed.	DE.CM-4
11.12.6	Anti-Malware software **must** be configured to disinfect, delete, quarantine or encrypt malware upon detection. Encryption of the malware **must** be reversible in the case of false positive detection (i.e. an XOR of the file is generally sufficient).	DE.CM-4
11.12.7	Anti-Malware software **must** be configured to automatically update signature or definition files in near real-time from a centralised internal source and from the Internet directly as a fall-back mechanism.	DE.CM-4
11.12.8	Anti-Malware software **must** be running the latest version of the underlying detection engine as well as the signature or definition files.	DE.CM-4

11.12.9	Anti-Malware software procurement and deployment processes must consider the use of heuristic scanning methods as well as traditional signature or definition-based scanning.	DE.CM-4
11.12.10	Anti-Malware software **must** be periodically verified for integrity. Ideally this verification check **must** be managed via a centralised console and adequately monitored. The meaning of integrity is that the service/ process associated with the software is running, the software remains tamper proof, the file and folder scanning exceptions are as expected, the efficacy of the detection engine is reviewed, and the signature or definition files are being updated as expected.	DE.CM-4 PR.DS-6
11.12.11	Anti-Malware Software **must** have its resource management options appropriately configured to ensure that CPU, memory and hard disk usage are never exhausted during operation	DE.CM-4

11.13 Content Inspection and Defence in Depth

Reference	Minimum Technical Security Measures	
11.13.1	Any standard users **must** be subject to a whitelisting and blacklisting URL reputation	PR.DS-5

	service for inspection for outbound Internet Browsing	
11.13.2	URL blacklisting reputational feeds for Internet Browsing **must** be updated in as near to real-time as operationally feasible on the Content Inspection boundary devices such as Next Generation Firewalls, Proxy Servers, or Web Content Filtering gateways referenced by the Internet Browsing boundary routers	PR.DS-5
11.13.3	URL blacklisting and Content Inspection for Internet Browsing **must** work in a blocking state for known malicious sites. In other words, URL blacklisting Content Inspection **must not** work in an “Inspect only” state for known malicious sites.	PR.DS-5
11.13.4	Email Content Inspection **must** have a minimum two layers of Anti-Malware scan performed prior to persisting attachments to departmental resources. This will take the form of Email Content Inspection on the relevant Mail Gateway and on the desktop, server or mobile endpoints Anti-Malware software inspection engine.	DE.CM-4
11.13.5	Intrusion Prevention systems (IPS) **must** be configured and maintained with the latest signatures and rule sets to help mitigate malware intrusion attempts and Indicators of Compromise, including blocking outbound command-and-control traffic.	DE.CM-4

11.13.6	Content Inspection technology capable of operating in an active blocking mode, (rather than only inspecting content), **must** have a clear and tested set of procedures to overcome false positives that may affect legitimate business processing. Block mode **must** be set after the initial installation and learning phases are completed.	DE.CM-4
11.13.7	Consideration **must** be given to complementary endpoint agent-based Defence in Depth technologies, e.g., Next Generation Anti-Malware Software (in addition to traditional Anti-Malware Software), host-based firewalls / intrusion prevention software and micro-virtualisation technologies.	DE.CM-4
11.13.8	Consideration **must** be given to complementary agentless Defence in Depth technologies such as Isolation and Rendering technologies, Sandboxing technologies and Data Science based solutions to help identify Indicators of Compromise.	DE.CM-4

11.14 Log Configuration and Collection

Reference	Minimum Technical Security Measures	
11.14.1	Anti-Malware Software on every operational endpoint **must** be configured to log any disinfection, deletion, quarantine or encryption	DE.CM-4

	actions in near real-time to a centrally managed console for the Anti-Malware Software in use. Where near real-time logging is not possible, digest logging **must** be configured.	
11.14.2	The Anti-Malware Centralised Console **must** be configured to forward in near real-time or in a digest format, logs aggregated from the clients it manages to a centralised SIEM system.	DE.CM-4
11.14.3	Any systems deployed for Content Inspection and Defence in Depth **must** have detection, inspection, blocking, quarantine, deletion, disinfection, traffic, and any encryption logs configured to forward to the centralised SIEM.	DE.CM-4 DE.DP-2 DE.DP-4
11.14.4	Configuration changes to operating parameters of any Anti-Malware technology including changes to logging facilities, administrative access, rule creation, and any content inspection updates **must** be tamper proof and logged either in near real-time or digested format to the centralised SIEM. This statement applies equally to system-initiated and system administrator changes to operating parameters including, exception modification, privilege access modifications and rule creation.	PR.IP-3
11.14.5	Separation of system administration duties **must** ensure that management of the centralised SIEM **does not** overlap with those privileged users supporting Malware protection services.	PR.AC-4

11.15 Log review and analysis

Reference	Minimum Technical Security Measures	
11.15.1	Baseline Management Information of the Anti-Malware Software logs and the Defence in Depth system logs **must** be validated, reconciled and processed for monthly reporting. This process **must** include the removal of any false positives.	PR.IP-1
11.15.2	A quarterly review (more frequently if required) of trending data collected via Anti-Malware Software and Defence in Depth logs **must** be performed. The review **must** establish any trends in the threat landscape highlighting any monthly changes. This can both validate and act as a complementary data source for other threat intelligence sources.	PR.IP-1

12. Appendices

Appendix A - Security Outcomes

The minimum security measures defined in this standard contribute to the achievement of security outcomes described in the table below. For consistency, the official NIST Sub-category IDs have been carried through to the standards.

Table 2 – List of Security Outcomes Mapping

Ref	Security Outcome (sub-category)	Related Security measure
ID.AM-1	Physical devices and systems within the organization are inventoried	11.3.2
ID.AM-2	Software platforms and applications within the organization are inventoried	11.3.1, 11.3.2
ID.AM-5	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	11.1.1
ID.BE-4	Dependencies and critical functions for delivery of critical services are established	11.1.2
ID.RA-1	Asset vulnerabilities are identified and documented	11.1.1
ID.RA-3	Threats, both internal and external, are identified and documented	11.11.1
ID.SC-3	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	11.1.2
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	11.2.2, 11.2.3, 11.4.1 11.4.2, 11.5.1, 11.5.2 11.5.3, 11.5.4, 11.5.5 11.9.1, 11.14.4
PR.AT-1	All users are informed and trained	11.5.1
PR.AT-2	Privileged users understand their roles and responsibilities	11.2.1
PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition	11.6.1, 11.6.2

PR.DS-5	Protections against data leaks are implemented	11.6.1, 11.6.2, 11.8.1 11.13.1, 11.13.2, 11.13.3
PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity	11.12.10
PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	11.15.1, 11.15.2
PR.IP-2	A System Development Life Cycle to manage systems is implemented	11.9.3, 11.9.4
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	11.4.3
PR.PT-4	Communications and control networks are protected	11.4.1, 11.4.2, 11.8.2
DE.CM-1	The network is monitored to detect potential cybersecurity events	11.7.2
DE.CM-4	Malicious code is detected	11.7.1, 11.7.2, 11.8.2 11.9.2, 11.10.1, 11.10.2, 11.10.3 11.12.1, 11.12.2 11.12.3, 11.12.4 11.12.5, 11.12.6 11.12.7, 11.12.8 11.12.9, 11.12.10 11.12.11, 11.13.4 11.13.5, 11.13.6 11.13.7, 11.13.8 11.14.1, 11.14.2 11.14.3
DE.CM-5	Unauthorized mobile code is detected	11.7.1, 11.7.2
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	11.7.1, 11.7.2
DE.DP-2	Detection activities comply with all applicable requirements	11.14.1
DE.DP-3	Detection processes are tested	11.7.1, 11.7.2

DE.DP-4	Event detection information is communicated	11.14.1

Appendix B - Internal references

Below is a list of internal documents that **should** be read in conjunction with this standard.

Table 3 – Internal References

Ref	Document	Publicly Available*
A	SS-010 Desktop Operating System Security Standard	Yes
B	SS-033 Security Patching Standard	Yes
C	SS-001 pt.2 Privileged User Access Security Standard	Yes

Requests to access non-publicly available documents **should be made to the Authority Contracts/Supplier Manager.*

Appendix C - External references

The following publications and guidance were considered in the development of this standard and **should** be referred to for further guidance.

Table 4 – External References

External Documents List
NIST Cyber Security Framework
CIS Critical Security Controls v8 controls set
OWASP Open Web Application Security Project

Appendix D - Abbreviations

Table 5 – Abbreviations

Abbreviation	Definition	Owner
CIS	Centre for Internet Security	Industry body
CMDB	Configuration Management Database	Industry term
CVE	Common Vulnerabilities and Exposures	Industry term
DWP	Department for Work and Pensions.	UK Government
GSCP	Government Security Classification Policy	UK Government
HID	Human Interface Devices	Industry term
IDS	Intrusion Detection System	Industry term
iFrames	Inline Frames	Industry term
IPS	Intrusion Prevention System	Industry term
ISO	International Organization for Standardization	Industry term
MAC	Mandatory Access Control	Industry term
NIST	National Institute of Standards and Technology	US Government
NIST – CSF	National Institute of Standards and Technology – Cyber Security Framework	US Government
OS	Operating System	Industry term
OWASP	Open Web Application Security Project	Open source
OWASP ASVS	(OWASP) Application Security Verification Standard	Open source
RDP	Remote Desktop Protocol	Industry term
SIEM	Security Incident Event Management	Industry term
SLA	Service Level Agreement	Industry term

Abbreviation	Definition	Owner
SSH	Secure Shell	Industry term
VPN	Virtual Private Network	Industry term

Appendix E - Glossary

Table 6 – Glossary

Term	Definition

Appendix F - Accessibility artefacts

A variety of accessibility guidance is available from the below URL, that includes:

https://www.gov.uk/guidance/guidance-and-tools-for-digital-accessibility

https://www.gov.uk/guidance/accessibility-requirements-for-public-sector-websites-and-apps